

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TENNESSEE

STATE OF TENNESSEE

COUNTY OF SHELBY

Case No. 22-SW-288

ATTACHMENT C

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, **Keyotta Sanford**, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the FBI assigned to the Memphis Division and have been a Special Agent since January 2019. I am currently assigned to the Child Exploitation & Human Trafficking Task Force, investigating matters involving the sexual exploitation of children, human trafficking, and child sexual abuse material (CSAM). I have participated in various trainings and investigations involving online and computer related offenses and have executed numerous search warrants, including those involving searches and seizure of computers, digital media and electronically stored information.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination and analysis of data for electronic devices, described in **Attachment A**, that currently are in possession of the Memphis Police Department, including the forensic extraction, examination, and review of electronically stored information as described in **Attachment B**.

3. You affiant is investigating certain activities in violation of 18 U.S.C § 1591 (sex trafficking by force, fraud, or coercion) and 18 U.S.C. § 2422(a) (coercion and enticement). Based

on my training and experience, and facts as set forth in this affidavit, there is probable cause to believe that items which constitute instrumentalities, fruits, and evidence of the aforementioned violations of will be found on the devices and electronically stored information described in **Attachments A and B.**

4. The following information was obtained through the assistance of other law enforcement agents and agencies, including their reports, and through other sources specifically named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. § 1591 and 18 U.S.C. § 2422(a) will be found on the devices described in **Attachment A**, and electronically stored information will consist of or be contained in the items listed in **Attachment B**, both of which are incorporated by reference as if fully set forth herein.

APPLICABLE STATUTES

5. Title 18, United States Code, Section 1591 makes it a federal offense for anyone, using a means of interstate or foreign commerce, to knowingly recruit, entice, harbor, transport, provide, obtain, advertise, maintain, patronize, or solicit by any means a person to engage in a commercial sex act or receive anything of value from participating in such a venture, through means of force, threats of force, fraud, coercion or any combination of such means.

6. Title 18, United States Code, Section 2422(a) makes it a federal offense for anyone to knowingly persuade, induce, entice, or coerce any individual to travel in interstate or foreign

commerce, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

DEFINITIONS

7. The following definitions apply to this affidavit and **Attachment B**:
 - a. As it is used in 18 U.S.C. § 1591, the term "coercion", is defined in 18 U.S.C. § 1591(e) as "threats of serious harm to or physical restraint against any person; any scheme, plan or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person or; the abuse or threatened abuse of law or the legal process".
 - b. The term "commercial sex act," as used herein, is defined pursuant to Title 18 U.S.C. § 1591(e) as "any sex act, on account of which anything of value is given to or received by any person."
 - c. As it is used in 18 U.S.C. § 1591, the term "serious harm" is defined in 18 U.S.C. § 1591(e) as any harm, "whether physical or nonphysical, including psychological, financial, or reputational harm, that is sufficiently serious, under all the surrounding circumstances, to compel a reasonable person of the same background and in the same circumstances to perform or to continue performing commercial sexual activity in order to avoid incurring that harm".
 - d. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number,

date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

e. A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

f. An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state

COMMERCIAL SEX TRAFFICKING, THE INTERNET & CELL PHONES

8. Based on my knowledge, training, and experience, and the experience and training of other law enforcement officers in child exploitation and human trafficking investigations with whom I have had discussions, I know that the Internet contains many website that are used to aid and assist in the advertising of prostitution. I also know it is common for those involved in Internet based sex trafficking to exclusively utilize cellular telephones to run their prostitution enterprise. An Internet connected mobile device can be used to take pictures and/or videos, generate advertisements, upload images, and solicit or receive payments electronically. I know that these activities can be detectable through a forensic examination of the device.

9. Additionally, I know it to be common for someone involved in commercial sex exploitation to maintain contact with the victim. When not physically together, a mobile phone becomes the primary method of communication. Not only can the “pimp” maintain control over the victim, this method of communication is also practical in the directing the victim to prostitute. For example, the “pimp” is able to tell the victim when to post ads, when and where to be for a “date”, how much to charge, and can also control the victim’s response. I know that more likely than not persons involved in trafficking women in prostitution related activities will contact those involved women via cell phone to discuss specific prostitution dates, availability and other prostitution related issues.

10. I know from my training and experience investigating similar crimes that these communications providing evidence of the crime will, more likely than not, be found within 30 days preceding the crime through 30 days after the crime. Communications about the crime involving the plotting, planning and execution, will more likely than not, be found within the 30 days preceding the crime and through the date of the crime while communications after the crime involving discussions of the sale, profits, proceeds and concealment will, more likely than not, be found within 30 days after the commission of the crime.

11. Furthermore, persons committing these criminal acts will, more likely than not, possesses images or videos depicting the girl(s) that are associated with prostitution or sex trafficking. I know from my training and experience investigating similar crimes that these images, videos, audio files and media providing evidence of the crime will, more likely than not, be found within 30 days preceding the crime through 30 days after the crime. Images, videos, audio files and media about the crime involving the plotting, planning and execution will, more likely than not, be found within the 30 days preceding the crime and through the date of the

crime while images, videos, audio files and media about the crimes after crime involving the sale, profits, proceeds and concealment will, more likely than not, be found with 30 days after the commission of the crime.

12. I know that cell phones have the capability to browse the Internet and such browsing history is stored within the memory of the phone. I further know based on my training and experience that persons committing offenses described herein will, more likely than not, possess evidence of their criminal acts within their cell phone Internet browsing history. Such evidence includes searching or posting advertisements on escort based websites; such as www.skipthegames.com and www.megapersonals.eu.

13. Based on my knowledge and experience, I know there are instances in which a “pimp” or trafficker will pose as the prostitution provider or victim and will have text message conversations directly with the potential prostitution “john” using their cell phone. The pimp or trafficker will discuss and arrange the prostitution “date” with the potential “john” via text message will posing as the prostitution provider or victim. It is also common that the pimp or trafficker will have a sexual relationship with their prostitution provider or victim. As such, the “pimp” or trafficker will take and store sexually explicit photos and/or videos of the victim on their cell phone(s), which may or may not be observed on escort websites.

INVESTIGATION

14. The devices are currently in the lawful possession of the Memphis Police Department and were obtained pursuant a State of Tennessee search warrant. Your affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the devices will comply with the Fourth Amendment and other applicable laws.

15. On September 23, 2022, the Memphis Police Department (MPD) responded to an intimidation call at the Econo Lodge Inn and Suites located at 6045 Macon Cv., Memphis, TN 38134. The complainant, hereby referred to as KL, reported to officers that Terrance Howard had threatened to physically harm her and when he could not enter her hotel room, he took the keys to her car and left the hotel prior to police arriving. KL further advised officers that she was being “pimped out” by Howard and had been forced to engage in commercial sex acts in not only in Tennessee, but also in other states. KL was prevented from leaving the situation due to Howard’s physical abuse and threats, but also due to the fact that he had taken her car keys and personal cell phone. While officers were on scene, Howard arrived at the hotel with another woman, later identified as G. Tipton, and both were subsequently detained. Officers were provided verbal consent by Tipton to search the vehicle, where they located the KL’s car key, which was broken, and a cell phone. The cellphone was later identified as belonging to Tipton and was described as a black Samsung Galaxy SM-G988U with a floral case. Officer’s seized two cellular phones from Howard’s person, which were described as a black iPhone with a black and silver case and a blue colored Android phone, which appeared to be a Blu View 3.

16. On 9/24/2022, your affiant and detectives with the MPD Internet Crimes Against Children unit interviewed KL who advised she met Howard approximately two or three months prior via the escort website www.megapersonals.eu. KL confided that prior to meeting Howard, she had started prostituting to make money approximately 7 months ago around the timeframe she had met her first “pimp”. KL accused Howard of manipulating her as he made her believe that he was not a “pimp” and had promised her a better life with him in Memphis, TN. KL traveled to Memphis, TN to be with Howard, and believed that they were in a romantic relationship. After approximately month, it became apparent to KL that Howard expected her to start working for

him.

17. According to KL, Howard's rules for her were "Don't Talk Back" and to "Act Right". When asked what the rules meant, KL further explained that he wanted her to not ask any questions and to shut up and just bring the money. Whenever she disobeyed he would say, "I'm going to show you," which was usually a precursor to physical abuse. KL had been beaten by Howard many times, some of which included having a busted nose and being strangled around the neck.

18. KL had traveled with Howard to Nashville, TN, Evansville, IN, and Charlotte, NC to engage in commercial sex acts. When asked how much she made on average a day, KL advised she had made approximately \$300 to \$400 in Evansville, \$1000 in Memphis, and \$1500 in Charlotte. KL would sometimes be given money to pay for food, and other expenses, such as her car note and insurance. KL would pay Howard via her "work" CashApp. Howard would sometimes pay for the hotel rooms and sometimes he would require her to pay. There were also instances where Howard would get two separate rooms at the hotel or get a hotel nearby for himself.

19. KL confided to Investigators that things had gotten unbearable within the last month. Howard began demanding that she work more and would beat her if she spent too much money. There were also times in which he would not allow her to eat and demanded that she "act right" and work. Approximately 2 weeks ago, she begged him to take her to the health department as she was suffering from staph infection and also what she believed was a sexually transmitted disease. Howard took her to the health department; however, the health department was not equipped to assist with the staph infection and Howard refused to get her additional medical assistance.

20. When KL told him that she was fed up with his treatment, KL told her that his hand reached out further than she knew. He knew where she and her family were located and he would find her regardless of where she attempted to run. KL was fearful for her safety as Howard had beaten her many times and she believed he had the means to act upon his threats as an active member of the Piru street gang. KL concluded by identifying his personal phone as an iPhone and his “pimp” phone as a blue Android phone. KL provided consent to search her “hoe” phone which was provided to her by Howard. KL told Investigators that all of the evidence was on their phones.

21. On 9/24/2022, Howard was advised of his Miranda Rights and was interviewed by Investigators. Howard advised he knew KL was a prostitute when he initially met her through a partner. He further corroborated her claims that the two traveled to Charlotte, NC, Nashville, TN and her hometown located in Evansville, IN. Howard admitted that he had paid for her hotel room a few times, to include the most recent and liked to “lend” KL money to help her out. She would pay him back via CashApp. Howard also admitted to taking her to the health department for a possible spider bite. Howard denied being the owner of the blue Android phone; however, he refused to say whom the phone belonged.

22. On 9/24/2022, Tipton was interviewed by Investigators. Tipton advised her car had been disabled and Howard had dropped off a car for her to use, which was later identified by Investigators as belonging to KL. Tipton had traveled with Howard and a male relative of Howard’s to Houston, TX on the morning of 9/23/2022. When asked to identify the phones retrieved at the scene, Tipton identified her phone as a iPhone with a floral case. Tipton told Investigators that Howard had two phones, an iPhone and a blue Android phone.

23. On 9/24/2022, a State of Tennessee search warrant was issued for the phones seized from Howard and Tipton. These phones were identified by MPD as containing evidence of

commercial sex trafficking. A forensic examination was conducted on two of the devices seized. One the iPhone, MPD officers observed messages between Howard and KL which provided further proof that Howard was physically abusive and threatening her to engage in commercial sex acts or else he would “show her”. In addition, Howard appeared to receive funds via CashApp which were obtained from the sex “dates”.

24. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 1591 and 2422(a) have been committed, and evidence, instrumentalities and fruits of those violations are located at on devices further described in **Attachments A and B** of this affidavit.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge and experience, cellular phones can also be considered portable data storage devices which contain several data storage features contained in one device. I know that deleted photos or deleted text message can likely be retrieved from cell phones and valuable information cannot be obtained through cell phone records maintained by the cell phone provider. There are various applications which are intended to be installed on Smart phones. These third party applications are intended to communicate with the cell network, Internet, or the phone’s communication features. I know these applications can be used for monetary transactions, email, short message services (SMS), Multi-Media Services (MMS) and for placing Internet-based phone calls. I know based on my training and experience that data found in the databases of installed applications are relevant to criminal investigations.

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the Subject device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -that is, in space on the storage medium that is not currently being used by an active file -for long periods of time before they are overwritten. In addition, a computer’s operating system also may keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media - in particular, computers’ internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or

delete this evidence, because special software is typically required for that task.

However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to participate or promote sex trafficking by force, fraud, or coercion, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain the following: data that is evidence of how the electronic device

was used; data that was sent or received; and other records that indicate the nature of the offenses and identity of the perpetrator(s).

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the court to authorize execution of the warrant at any time in the day or night.

JURISDICTION

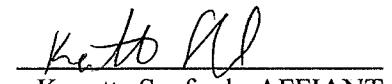
31. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

32. I believe that based upon the totality of facts and circumstances described above, probable cause exists to search the device described above for evidence and instrumentalities of and concerning violations of 18 U.S.C. § 1591 and 18 U.S.C. § 2422(a). In consideration of the foregoing, your affiant respectfully requests that this Court issue a search warrant authorizing the

examination, analysis and review of the devices more specifically described in **Attachment A**, authorizing the search and seizure of the items described in **Attachment B**, incorporated herein.

AND FURTHER, AFFIANT SAITH NOT.


Keyotta Sanford - AFFIANT
Special Agent,
Federal Bureau of Investigation.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 30th day of September, 2022.


HON. ANNIE T. CHRISTOFF
United States Magistrate Judge